# PART 2400—REGULATIONS TO IMPLEMENT E.O. 12356; OFFICE OF SCIENCE AND TECHNOLOGY POLICY INFORMATION SECURITY PROGRAM

## Subpart A—General Provisions



## Subpart B—Original Classification



## Subpart C—Derivative Classification



## Subpart D—Declassification and Downgrading



## Subpart E—Safeguarding



## Subpart F—Foreign Government Information



## Subpart G—Security Education



## Subpart H—Office of Science and Technology Policy Information Security Program Management



AUTHORITY: E.O. 12356 and Information Security Oversight Office Directive No. 1.

SOURCE: 48 FR 10821, Mar. 15, 1983, unless otherwise noted.

## Subpart A—General Provisions

### § 2400.1 Authority.

(a) Executive Order 12356 ''National Security Information,'' dated April 2, 1982, 47 FR 14874 (Apr. 6, 1982); 47 FR 15557 (Apr. 12, 1982) and Order of Designation of May 7, 1982, 47 FR 20105 (May 11,1982).

(b) Information Security Oversight Office, Directive No. 1, ''National Security Information,'' dated June 23, 1982, 47 FR 27836 (June 25, 1982) (Directive No. 1).

### § 2400.2 Purpose.

The purpose of this Regulation is to ensure, consistent with the authorities of § 2400.1 that information of the Office of Science and Technology Policy (OSTP) relating to national security is protected from unauthorized disclosure, but only to the extent and for such period as is necessary to safeguard the national security.

### § 2400.3 Applicability.

This Regulation governs the Office of Science and Technology Policy Information Security Program. In accordance with the provisions of Executive Order 12356 and Directive No. 1 it establishes, for uniform application throughout the Office of Science and Technology Policy, the policies and procedures for the security classification, downgrading, declassification and safeguarding of information that is owned by, produced for or by, or under the control of the office of Science and Technology Policy.

### § 2400.4 Atomic Energy Material.

Nothing in this Regulation supersedes any requirement made by or under the Atomic Energy act of 1954, as amended. ''Restricted Data'' and information designated as ''Formerly Restricted Data'' shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued pursuant thereto by the Department of Energy.

## Subpart B—Original Classification

### § 2400.5 Basic policy.

Except as provided in the Atomic Energy Act of 1954, as amended, Executive Order 12356, as implemented by Directive No. 1 and this Regulation, provides the only basis for classifying information. The policy of the Office of Science and Technology Policy is to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security. Information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security.

### § 2400.6 Classification levels.

(a) National security information (hereinafter ''classified information'') shall be classified at one of the following three levels:

(1) ''Top Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) ''Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) ''Confidential'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information. Markings other than ''Top Secret,'' ''Secret,'' and ''Confidential,'' such as ''For Official Use Only,'' shall not be used to identify national security information. In addition, no other term or phrase shall be used in conjunction with one of the three authorized classification levels, such as ''Secret Sensitive'' or ''Agency Confidential.'' The terms ''Top Secret'', ''Secret'', and ''Confidential'' should not be used to identify nonclassified executive branch information.

(c) Unnecessary classification, and classification at a level higher than is necessary shall be scrupulously avoided.

(d) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified ''Confidential'' pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification the originator of the information shall safeguard it at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days. Upon the determination of a need for classification and/or the proper classification level, the information that is classified shall be marked as provided in § 2400.12 of this part.

### § 2400.7 Original classification authority.

(a) Authority for original classification of information as Top Secret shall be exercised within OSTP only by the

Director and by such principal subordinate officials having frequent need to exercise such authority as the Director shall designate in writing.

(b) The authority to classify information originally as Secret shall be exercised within OSTP only by the Director, other officials delegated in writing to have original Top Secret classification authority, and any other officials delegated in writing to have original Secret classification authority.

(c) The authority to classify information originally as Confidential shall be exercised within OSTP only by officials with original Top Secret or Secret classification authority and any officials delegated in writing to have original Confidential classification authority.

### §2400.8 Limitations on delegation of original classification authority.

(a) The Director, OSTP is the only official authorized to delegate original classification authority.

(b) Delegations of original classification authority shall be held to an absolute minimum.

(c) Delegations of original classification authority shall be limited to the level of classification required.

(d) Original classification authority shall not be delegated to OSTP personnel who only quote, restate, extract or paraphrase, or summarize classified information or who only apply classification markings derived from source material or as directed by a classification guide.

(e) The Executive Director, OSTP, shall maintain a current listing of persons or positions receiving any delegation of original classification authority. If possible, this listing shall be unclassified.

(f) Original classification authority may not be redelegated.

(g) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of OSTP that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with these Regulations as provided in §2400.6(d) of this part. The information shall be transmitted promptly as provided in these Regulations to the official in OSTP who has appropriate subject matter interest and classification authority with respect to this information. That official shall decide within thirty (30) days whether to classify this information. If the information is not within OSTP's area of classification responsibility, OSTP shall promptly transmit the information to the responsible agency. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

### §2400.9 Classification requirements.

(a) Information may be classified only if it concerns one or more of the categories cited in Executive Order 12356, as subcategorized below, *and* an official having original classification authority determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(1) Military plans, weapons or operations;

(2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) Foreign government information;

(4) Intelligence activities (including special activities), or intelligence sources or methods;

(5) Foreign relations or foreign activities of the United States;

(6) Scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safe-guarding nuclear materials or facilities;

(8) Cryptology;

(9) A confidential source; or

(10) Other categories of information which are related to national security and that require protection against unauthorized disclosure as determined by the Director, Office of Science and Technology Policy. Each such determination shall be reported promptly to

the Director of the Information Security Oversight Office.

(b) Foreign government information need not fall within any other classification category listed in paragraph (a) of this section to be classified.

(c) Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be fully supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

(d) Information classified in accordance with this section shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information. Following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with Executive Order 12356 or predecessor orders, OSTP, if the agency of primary interest, shall determine the degree of damage to the national security, the need for continued classification, and in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences. If the agency of primary interest is other than OSTP, the matter shall be referred to that agency.

### § 2400.10 Presumption of damage.

Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods, is presumed to cause damage to the national security.

### § 2400.11 Duration of classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor Executive Orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The originating agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor Executive Orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of Executive Order 12356.

(d) Information classified under predecessor Executive Orders that does not bear a specific date or event for declassification shall remain classified until reviewed for declassification. The authority to extend the classification of information subject to automatic declassification under predecessor Orders is limited to those officials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Director of the Information Security Oversight Office.

### § 2400.12 Identification and markings.

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

(1) One of the three classification levels defined in § 2400.6 of this part;

(2) The identity of the original classification authority if other than the person whose name appears as the approving or signing official;

(3) The agency and office of origin; and

(4) The date or event for declassification, or the notation ''Originating Agency's Determination Required.''

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. The Director OSTP may, for good cause,

grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of Executive Order 12356, including abbreviations, shall conform to the standards prescribed in Directive No. 1 issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor Executive Orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in §2400.18 of this part.

### §2400.13 Limitations on classification.

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) The Director may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office. Before reclassifying any information, the Director shall consider the factors listed in §2001.6 of Directive No. 1, which shall be addressed in the report to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after OSTP has received a request for it under the Freedom of Information Act (5 U.S.C. 552a) or the Privacy Act of 1974 (5 U.S.C. 552), or the mandatory review provisions of Executive Order 12356 (section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the Director.

## Subpart C—Derivative Classification

### §2400.14 Use of derivative classification.

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. If a person who applies derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult an appropriate official of the originating agency or office of origin who has the authority to declassify, downgrade or upgrade the information.

(b) Persons who apply derivative classification markings shall:

(1) Observe and respect original classification decisions; and

(2) Carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

### §2400.15 Classification guides.

(a) OSTP shall issue and maintain classification guides to facilitate the proper and uniform derivative classification of information. These guides shall be used to direct derivative classification.

(b) The classification guides shall be approved, in writing, by the Director or by officials having Top Secret original classification authority. Such approval

constitutes an original classification decision.

(c) Each classification guide shall specify the information subject to classification in sufficient detail to permit its ready and uniform identification and categorization and shall set forth the classification level and duration in each instance. Additionally, each classification guide shall prescribe declassification instructions for each element of information in terms of (1) a period of time, (2) the occurrence of an event, or (3) a notation that the information shall not be automatically declassified without the approval of OSTP.

(d) The classification guides shall be kept current and shall be fully reviewed at least every two years. The Executive Director, OSTP shall maintain a list of all OSTP classification guides in current use.

(e) The Executive Director, OSTP shall receive and maintain the record copy of all approved classification guides and changes thereto. He will assist the originator in determining the required distribution.

(f) The Director may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers. The Director's decision to waive the requirement to issue classification guides for specific classes of documents or information will be based, at a minimum, on an evaluation of the following factors:

(1) The ability to segregate and describe the elements of information;

(2) The practicality of producing or disseminating the guide because of the nature of the information;

(3) The anticipated usage of the guide as a basis for derivative classification; and

(4) The availability of alternative sources for derivatively classifying the information in a uniform manner.

### § 2400.16 Derivative classification markings.

(a) Documents classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2400.12 of this part and Directive No. 1 as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide. When markings are omitted because they may reveal a confidential source or relationship not otherwise evident, as described in § 2400.12 of this part, the information may not be used as a basis for derivative classification.

(b) The authority for classification shall be shown as directed in Directive No. 1.

## Subpart D—Declassification and Downgrading

### § 2400.17 Policy.

Declassification of information shall be given emphasis comparable to that accorded classification. Information classified pursuant to Executive Order 12356 and prior orders shall be declassified or downgraded as soon as national security considerations permit. Decisions concerning declassification shall be based on the loss of sensitivity of the information with the passage of time or on the occurrence of an event which permits declassification. When information is reviewed for declassification pursuant to this regulation, that information shall be declassified unless the designated declassification authority determines that the information continues to meet the classification requirements prescribed in § 2400.9 of this part despite the passage of time. The Office of Science and Technology Policy officials shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter.

### § 2400.18 Declassification and downgrading authority.

Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the Director, OSTP. The Executive Director, OSTP shall maintain a current listing of persons or positions receiving

those delegations. If possible, these listings shall be unclassified.

### § 2400.19 Declassification by the Director of the Information Security Oversight Office.

If the Director of the Information Security Oversight Office (ISOO) determines that information is classified in violation of Executive Order 12356, the Director, ISOO may require the information to be declassified by the agency that originated the classification. Any such decision by the Director ISOO may be appealed by the Director, OSTP to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

### § 2400.20 Systematic review for declassification.

(a) *Permanent records.* Systematic review is applicable only to those classified records, and presidential papers or records that the Archivist of the United States, acting under the Federal Records Act, has determined to be of sufficient historical or other value to warrant permanent retention.

(b) *Non-permanent records.* Non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services under the Records Disposal Act. These schedules shall provide for the continued retention of records subject to an ongoing mandatory review for declassification request.

(c) *Office of Science and Technology Policy Responsibility.* The Director, OSTP, shall:

(1) Issue guidelines for systematic declassification review and, if applicable, for downgrading. These guidelines shall be developed in consultation with the Archivist and the Director of the Information Security Oversight Office and be designated to assist the Archivist in the conduct of systematic reviews;

(2) Designate experienced personnel to provide timely assistance to the Archivist in the systematic review process;

(3) Review and update guidelines for systematic declassification review and downgrading at least every five years unless earlier review is requested by the Archivist.

(d) *Foreign Government Information.* Systematic declassification review of foreign government information shall be in accordance with guidelines issued by the Director of the Information Security Oversight Office.

(e) *Special procedures.* The Office of Science and Technology Policy shall be bound by the special procedures for systematic review of classified cryptologic records and classified records pertaining to intelligence activities (including special activities) or intelligence sources or methods issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

### § 2400.21 Mandatory review for declassification.

(a) Except as provided in paragraph (d) of this section, all information classified under Executive Order 12356 or predecessor orders shall be subject to a review for declassification by the Office of Science and Technology Policy, if:

(1) The request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and

(2) The request is made in writing and describes the document or material containing the information with sufficient specificity to enable the Office of Science and Technology Policy to locate it with a reasonable amount of effort.

(b) Requests should be addressed to: Executive Director, Office of Science and Technology Policy, Executive Office of the President, Washington, DC 20506.

(c) If the request does not reasonably describe the information sought to allow identification of documents containing such information, the requester shall be notified that unless additional information is provided or the request is made more specific, no further action will be taken.

(d) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a

President is exempted from the mandatory review provisions of § 2400.24(a) of this part. The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matters interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(e) Office of Science and Technology Policy officials conducting a mandatory review for declassification shall declassify information no longer requiring protection under Executive Order 12356. They shall release this information unless withholding is otherwise authorized under applicable law.

(f) Office of Science and Technology Policy responses to mandatory review requests shall be governed by the amount of search and review time required to process the request. Normally the requester shall be informed of the Office of Science and Technology Policy determination within thirty days of receipt of the original request (or within thirty days of the receipt of the required amplifying information in accordance with paragraph (c) of this section). In the event that a determination cannot be made within thirty days, the requester shall be informed of the additional time needed to process the request. However, OSTP, shall make a final determination within one year from the date of receipt of the request except in unusual circumstances.

(g) When information cannot be declassified in its entirety, OSTP will make a reasonable effort to release, consistent with other applicable law, those declassified portions of that requested information the constitute a coherent segment.

(h) If the information may not be released in whole or in part, the requester shall be given a brief statement as to the reason for denial, and notice of the right to appeal the determination in writing within sixty days of receipt of the denial to the chairperson of the Office of Science and Technology Policy Review Committee. If appealed, the requester shall be informed in writing of the appellate determination within thirty days of receipt of the appeal.

(i) When a request is received for information originated by another agency, the Executive Director, Office of Science and Technology Policy, shall:

(1) Forward the request to such agency for review together with a copy of the document containing the information requested, where practicable, and where appropriate, with the Office of Science and Technology Policy recommendation to withhold or declassify and release any of the information;

(2) Notify the requester of the referral unless the agency to which the request is referred objects to such notice on grounds that its association with the information requires protection; and

(3) Request, when appropriate, that the agency notify the Office of Science and Technology Policy of its determination.

(j) If the request requires the rendering of services for which fees may be charged under title 5 of the Independent Offices Appropriation Act, 31 U.S.C. 483a, the Executive Director, Office of Science and Technology Policy, may calculate the anticipated amount of fees to be charged.

(1) Fees for the location and reproduction of information that is the subject of a mandatory review request shall be assessed according to the following schedule:

(i) *Search for records.* $5.00 per hour when the search is conducted by a clerical employee; $8.00 per hour when the search is conducted by a professional employee. No fee shall be assessed for searches of less than one hour.

(ii) *Reproduction of documents.* Documents will be reproduced at a rate of

$.25 per page for all copying of four pages or more. No fee shall be assessed for reproducing documents that are three pages or less, or for the first three pages of longer documents.

(2) Where it is anticipated that the fees chargeable under this section will amount to more than $25, and the requestor has not indicated in advance a willingness to pay fees as high as are anticipated, the requester shall be promptly notified of the amount of the anticipated fee or such portion thereof as can readily be estimated. In instances where the estimated fees will greatly exceed $25, an advance deposit may be required. Dispatch of such a notice or request shall suspend the running of the period for response by OSTP until a reply is received from the requester.

(3) Remittances shall be in the form either of a personal check or bank draft drawn on a bank in the United States, or a postal money order. Remittances shall be made to the Treasury of the United States and mailed to the Executive Director, Office of Science and Technology Policy, Executive Office of the President, Washington, DC 20506.

(4) A receipt for fees paid will be given only upon request. Refund of fees paid for services actually rendered will not be made.

(5) If a requester fails to pay within thirty days for services rendered, further action on any other requests submitted by that requestor shall be suspended.

(6) The Executive Director, Office of Science and Technology Policy may waive all or part of any fee provided for in this section when it is deemed to be in either the interest of the OSTP or the general public.

### §2400.22 Freedom of Information Act and Privacy Act requests.

The Office of Science and Technology Policy shall process requests for declassification that are submitted under the provisions of the Freedom of Information Act, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

### §2400.23 Prohibition.

In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of Executive Order 12356 and Directive No. 1, or this regulation:

(a) The Office of Science and Technology Policy shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under Executive Order 12356.

(b) When the Office of Science and Technology Policy receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases which the originating agency determines in writing that a response under paragraph (a) of this section is required, the Office of Science and Technology Policy shall respond to the requester in accordance with that paragraph.

### §2400.24 Downgrading.

(a) When it will serve a useful purpose, original classification authorities may, at the time of original classification, specify that downgrading of the assigned classification will occur on a specified date or upon the occurrence of a stated event.

(b) Classified information marked for automatic downgrading is downgraded accordingly without notification to holders.

(c) Classified information not marked for automatic downgrading may be assigned a lower classification designation by the originator or by an official authorized to declassify the same information. Prompt notice of such downgrading shall be provided to known holders of the information.

## Subpart E—Safeguarding

### §2400.25 Access.

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has

been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes. A personnel security clearance is an indication that the trustworthiness decision has been made. Procedures shall be established by the head of each office to prevent access to classified information before a personnel security clearance has been granted. The number of people cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs. No one has a right to have access to classified information solely by virtue of rank or position. The final responsibility for determinating whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests with the individual who has authorized possession, knowledge, or control of the information and not with the prospective recipient. These principles are equally applicable if the prospective recipient is an organizational entity, other Federal agencies, contractors, foreign governments, and others.

(b) When access to a specific classification category is no longer required for the performance of an individual's assigned duties, the security clearance will be administratively adjusted, without prejudice to the individual, to the classification category, if any, required.

(c) The Director, Office of Science and Technology Policy may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to Executive Order 12356 or predecessor orders if:

(1) Normal management and safeguarding procedures do not limit access sufficiently;

(2) The number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information;

(3) The special access program is established in writing; and

(4) A system of accounting for the program is established and maintained.

### § 2400.26 Access by historical researchers and former Presidential appointees.

(a) The requirement in Section 4.1(a) of Executive Order 12356 that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in paragraph (b) of this section for persons who:

(1) Are engaged in historical research projects, or

(2) Previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under paragraph (a) of this section may be granted only if the Director, Office of Science and Technology Policy:

(1) Determines in writing that access is consistent with the interest of national security;

(2) Takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with Executive Order 12356;

(3) Limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee; and

(4) Has received a written agreement from the researcher or former presidential appointee that his notes can be reviewed by OSTP for a determination that no classified material is contained therein.

### § 2400.27 Storage of classification information.

Whenever classified information is not under the personal control and observation of an authorized person, it will be guarded or stored in a locked security container approved for the storage and protection of the appropriate level of classified information as prescribed in § 2001.43 of Directive No. 1.

### § 2400.28 Dissemination of classified information.

Heads of OSTP offices shall establish procedures consistent with this Regulation for dissemination of classified material. The originating official may prescribe specific restrictions on dissemination of classified information when necessary.

(a) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(b) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

### § 2400.29 Accountability and control.

(a) Each item of Top Secret, Secret, and Confidential information is subject to control and accountability requirements.

(b) The Security Officer will serve as Top Secret Control Officer (TSCO) for the Office of Science and Technology Policy and will be responsible for the supervision of the Top Secret control program. He/she will be assisted by an Assistant Top Secret Control Officer (ATSCO) to effect the Controls prescribed herein for all Top Secret material.

(c) The TSCO shall receive, transmit, and maintain current access and accountability records for Top Secret information. The records shall show the number and distribution of all Top Secret documents, including any reproduced copies.

(d) Top Secret documents and material will be accounted for by a continuous chain of receipts.

(e) An inventory of Top Secret documents shall be made at least annually.

(f) Destruction of Top Secret documents shall be accomplished only by the TSCO or the ATSCO.

(g) Records shall be maintained to show the number and distribution of all classified documents covered by special access programs, and of all Secret and Confidential documents which are marked with special dissemination and reproduction limitations.

(h) The Security Officer will develop procedures for the accountability and control of Secret and Confidential information. These procedures shall require all Secret and Confidential material originated or received by OSTP to be controlled. Control shall be accomplished by the ATSCO.

### § 2400.30 Reproduction of classified information.

Documents or portions of documents and materials that contain Top Secret information shall not be reproduced without the consent of the originator or higher authority. Any stated prohibition against reproduction shall be strictly observed. Copying of documents containing classified information at any level shall be minimized. Specific reproduction equipment shall be designated for the reproduction of classified information and rules for reproduction of classified information shall be posted on or near the designated equipment. Notices prohibiting reproduction of classified information shall be posted on equipment used only for the reproduction of unclassified information. All copies of classified documents reproduced for any purpose including those incorporated in a working paper are subject to the same controls prescribed for the document from which the reproduction is made.

### § 2400.31 Destruction of classified information.

(a) Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of chapters 21 and 33 of title 44, U.S.C., which governs disposition of classified records. Classified information approved for destruction shall be destroyed in accordance with procedures and methods prescribed by the Director, OSTP, as implemented by the Security Officer. These procedures and methods must provide adequate protection to prevent access by unauthorized persons and must preclude recognition

or reconstruction of the classified information or material.

(b) All classified information to be destroyed will be provided to the ATSCO for disposition. Controlled documents will be provided whole so that accountability records may be corrected prior to destruction by the ATSCO.

### § 2400.32 Transmittal of classified information.

The transmittal of classified information outside of the Office of Science and Technology Policy shall be in accordance with procedures of § 2001.44 of Directive No. 1. The Security Officer shall be responsible for resolving any questions relative to such transmittal.

### § 2400.33 Loss or possible compromise.

(a) Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to the Security Officer. The Security Officer shall notify the Director and the agency that originated the information as soon as possible so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise.

(b) The Security Officer shall initiate an inquiry to:

(1) Determine cause,

(2) Place responsibility, and

(3) Take corrective measures and appropriate administrative, disciplinary, or legal action.

(c) The Security Officer shall keep the Director advised on the details of the inquiry.

## Subpart F—Foreign Government Information

### § 2400.34 Classification.

(a) Foreign government information classified by a foreign government or international organization of governments shall retain its original classification designation or be assigned a United States classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

(b) Foreign government information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that it be held in confidence must be classified because Executive Order 12356 states a presumption of damage to the national security in the event of unauthorized disclosure of such information.

### § 2400.35 Duration of classification.

Foreign government information shall not be assigned a date or event for automatic declassification unless specified or agreed to by the foreign entity.

### § 2400.36 Declassification.

Officials shall respect the intent of this Regulation to protect foreign government information and confidential foreign sources.

### § 2400.37 Mandatory review.

Except as provided in this paragraph, OSTP shall process mandatory review requests for classified records containing foreign government information in accordance with § 2400.21. The agency that initially received or classified the foreign government information shall be responsible for making a declassification determination after consultation with concerned agencies. If OSTP receives a request for mandatory review and is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request.

### § 2400.38 Protection of foreign government information.

Classified foreign government information shall be protected as is prescribed by this regulation for United States classified information of a comparable level.

## Subpart G—Security Education

### §2400.39 Responsibility and objectives.

The OSTP Security Officer shall establish a security education program for OSTP personnel. The program shall be sufficient to familiarize all OSTP personnel with the provisions of Executive Order 12356 and Directive No. 1, and this regulation. It shall be designed to provide initial, refresher, and termination briefings to impress upon them their individual security responsibilities.

## Subpart H—Office of Science and Technology Policy Information Security Program Management

### §2400.40 Responsibility.

The Director, OSTP is the senior OSTP official having authority and responsibility to ensure effective and uniform compliance with and implementation of Executive Order 12356 and its implementing Directive No. 1. As such, the Director, OSTP, shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the OSTP Information Security Program. The Director, OSTP, may approve waivers or exceptions to the provisions of this regulation to the extent such action is consistent with Executive Order 12356 and Directive No. 1.

### §2400.41 Office Review Committee.

The Office of Science and Technology Policy Review Committee (hereinafter referred to as the Office Review Committee) is hereby established and will be responsible for the continuing review of the administration of this Regulation with respect to the classification and declassification of information or material originated or held by the Office of Science and Technology Policy. The Office Review Committee shall be composed of the Executive Director who shall serve as chairperson, the Assistant Director for National Security & Space, and the Security Officer.

### §2400.42 Security Officer.

Under the general direction of the Director, the Special Assistant to the Executive Director will serve as the Security Officer and will supervise the administration of this Regulation. He/she will develop programs, in particular a Security Education Program, to insure effective compliance with and implementation of the Information Security Program. Specifically he/she also shall:

(a) Maintain a current listing by title and name of all persons who have been designated in writing to have original Top Secret, Secret, and Confidential Classification authority. Listings will be reviewed by the Director on an annual basis.

(b) Maintain the record copy of all approved OSTP classification guides.

(c) Maintain a current listing of OSTP officials designated in writing to have declassification and downgrading authority.

(d) Develop and maintain systematic review guidelines.

### §2400.43 Heads of offices.

The Head of each unit is responsible for the administration of this regulation within his area. These responsibilities include:

(a) Insuring that national security information is properly classified and protected;

(b) Exercising a continuing records review to reduce classified holdings through retirement, destruction, downgrading or declassification;

(c) Insuring that reproduction of classified information is kept to the absolute minimum;

(d) Issuing appropriate internal security instructions and maintaining the prescribed control and accountability records on classified information under their jurisdiction.

### §2400.44 Custodians.

Custodians of classified material shall be responsible for providing protection and accountability for such material at all times and particularly for locking classified material in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures which insure that unauthorized persons

do not gain access to classified information or material by sight or sound, and classified information shall not be discussed with or in the presence of unauthorized persons.

### § 2400.45 Information Security Program Review.

(a) The Director, OSTP, shall require an annual formal review of the OSTP Information Security Program to ensure compliance with the provisions of Executive Order 12356 and Directive No. 1, and this regulation.

(b) The review shall be conducted by a group of three to five persons appointed by the Director and chaired by the Executive Director. The Security Officer will provide any records and assistance required to facilitate the review.

(c) The findings and recommendations of the review will be provided to the Director for his determination.

### § 2400.46 Suggestions or complaints.

Persons desiring to submit suggestions or complaints regarding the Office of Science and Technology Policy Information Security Program should do so in writing. This correspondence should be addressed to: Executive Director, Office of Science and Technology Policy, Executive Office of the President, Washington, DC 20506.